Blocked!!!

How to react to having your network connection blocked!

Blocking Strategies

FNAL blocking strategies are broken into external and internal blocks. External blocks are applied at the Border Router and are done through Autoblocker, an automated tool. Internal Blocks are applied to systems vulnerable to bad guys, viri and worms, declared Critical Vulnerabilities and systems already infected (blocked by request of FCIRT). Infected systems that are blocked can not be unblocked without FCIRT approval!

AutoBlocker

An automated utility that places blocks at the border router. Outbound system behavior that triggers the Autoblocker:

- Multiple systems accessed in short time
- Multiple ports accessed on single system

Outbound block triggers E-mail to User or system administrator and to Nightwatch (Computer Security folk).

Autoblocker is usually triggered by infected (virus) systems, Peer-to-Peer file sharing, online gaming and web search engines scanning internal web sites. When the bad identified behavior stops, the block is automatically removed 30 minutes after the triggering behavior has stopped.

Internal Blocks

Computer Security runs automated scanners that check systems for critical vulnerabilities (http://computing.fnal.gov/security/CriticalVuln/). If a system is found with a critical vulnerability, mail is sent with the vulnerabilities found to the registered system administrator. A summary mail of systems with critical vulnerabilities is sent to Nightwatch twice a day.

Nightwatch manually selects candidates for blocking based on certain criteria:

- Immediate if multiple vulnerabilities
- Immediate if no contact or no E-mail address for system administrator
- Otherwise allow ~24 hours to fix problem after first time system is on list
- *To be automated in the future*

To have a system unblocked that has been manually blocked, the user **must** send mail to Nightwatch stating problem has been fixed and including identification of the system.

Please do this for nodes with critical vulnerabilities even if not blocked. Current block lists are checked manually by CST before unblocking. The list of Blocked nodes is at:

- http://www-dcn.fnal.gov/~netadmin/blocked/

Nightwatch sends a list of block/unblock nodes to Data Communications for processing twice a day (morning and afternoon) only (and only during work days now). *To be automated and running 24x7 in future.* Please note that nodes blocked Friday afternoon will **NOT** be unblocked until Monday morning!

In Summary

- Make sure someone is registered as system administrator with a valid E-mail address
- Promptly install the necessary patches or configuration changes
- Send mail to Nightwatch after correction and include identification of the system